

Introduction to P3P

Lorrie Faith Cranor

P3P Specification Working Group Chair
Carnegie Mellon University

May 2004

<http://lorrie.cranor.org/>

Privacy policies

- Policies let visitors know about site's privacy practices
- Visitors can then decide whether or not practices are acceptable, when to opt-in or opt-out, and who to do business with
- The presence of privacy policies increases trust

Privacy policy problems

■ BUT policies are often

- ★ difficult to understand
- ★ hard to find
- ★ take a long time to read
- ★ change without notice

Platform for Privacy Preferences Project (P3P)

- Developed by the World Wide Web Consortium (W3C) <http://www.w3.org/p3p/>
 - ★ Final P3P1.0 Recommendation issued 16 April 2002
- Offers an easy way for web sites to communicate about their privacy policies in a standard machine-readable format
 - ★ Can be deployed using existing web servers
- Enables the development of tools (built into browsers or separate applications) that
 - ★ Summarize privacy policies
 - ★ Compare policies with user preferences
 - ★ Alert and advise users

Basic components

- P3P provides a standard XML format that web sites use to encode their privacy policies
- Sites also provide XML “policy reference files” to indicate which policy applies to which part of the site
- Sites can optionally provide a “compact policy” by configuring their servers to issue a special P3P header when cookies are set
- No special server software required
- User software to read P3P policies called a “P3P user agent”

What's in a P3P policy?

- Name and contact information for site
- The kind of access provided
- Mechanisms for resolving privacy disputes
- The kinds of data collected
- How collected data is used, and whether individuals can opt-in or opt-out of any of these uses
- Whether/when data may be shared and whether there is opt-in or opt-out
- Data retention policy

Compact policies

- Provide very short summary of full P3P policy for cookies
- Not required
- Must be used in addition to full policy
- May only be used with cookies
- Must commit to following policy for lifetime of cookies
- May over simplify site's policy
- IE6 relies heavily on compact policies for cookie filtering - especially an issue for third-party cookies

Legal issues

- P3P specification does not address legal standing of P3P policies or include enforcement mechanisms
- P3P specification requires P3P policies **to be consistent** with natural-language policies
 - ★ P3P policies and natural-language policies are not required to contain the same level of detail
 - ★ Typically natural-language policies contain more detailed explanations of specific practices
- The same attorneys and policy makers involved in drafting natural-language privacy policy should be involved in creating P3P policy

Privacy policy

Designed to be read by a human

Can contain fuzzy language with “wobble room”

Can include as much or as little information as a site wants

Easy to provide detailed explanations

Sometimes difficult for users to determine boundaries of what it applies to and when it might change

Web site controls presentation

P3P policy

Designed to be read by a computer

Mostly multiple choice - sites must place themselves in one “bucket” or another

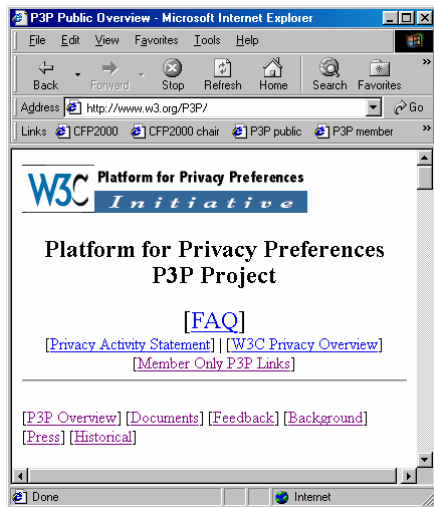
Must include disclosures in every required area

Limited ability to provide detailed explanations

Precisely scoped

User agent controls presentation

A simple HTTP transaction

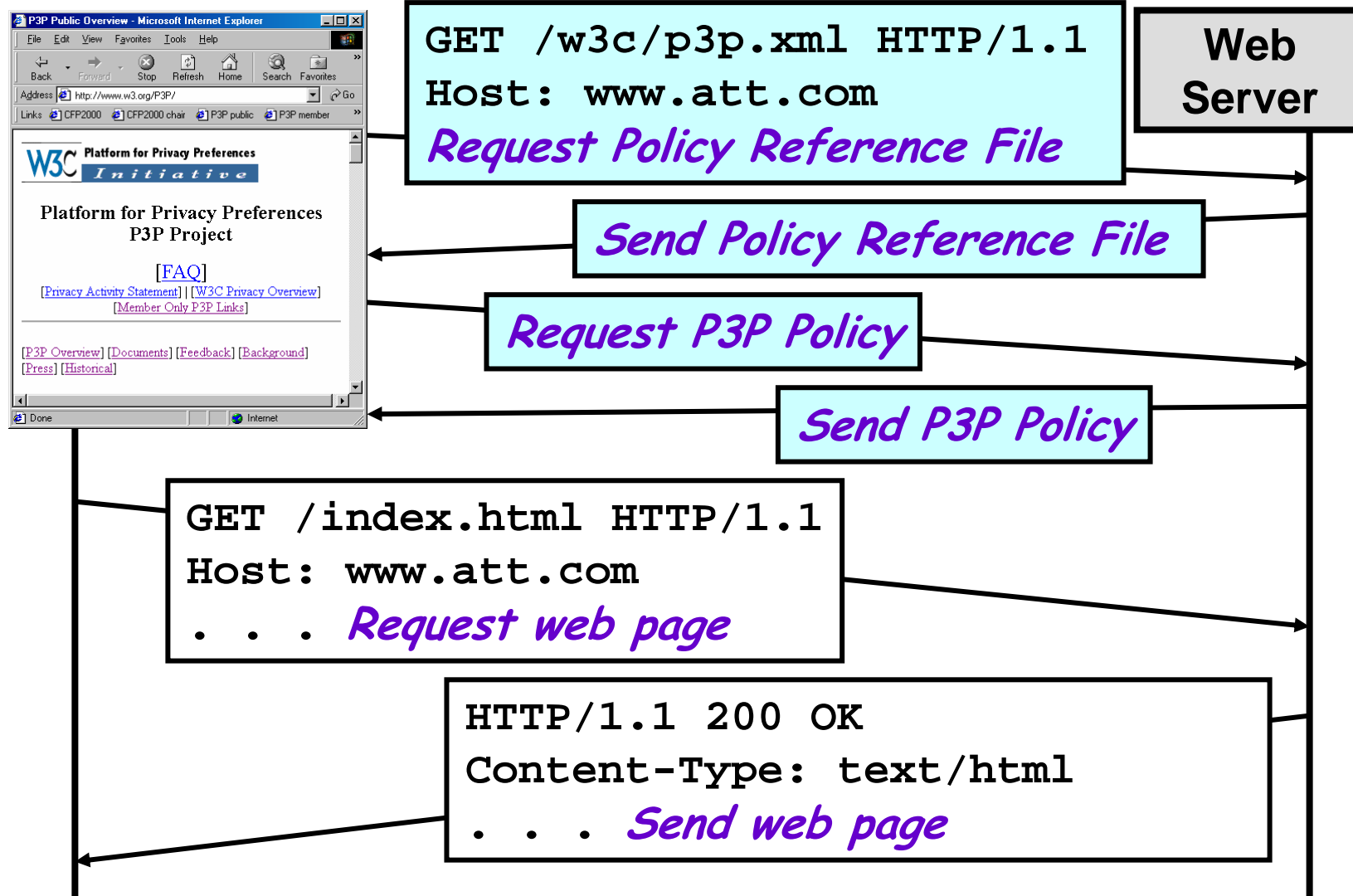


GET /index.html HTTP/1.1
Host: www.att.com
. . . *Request web page*

Web
Server

HTTP/1.1 200 OK
Content-Type: text/html
. . . *Send web page*

... with P3P 1.0 added



P3P increases transparency

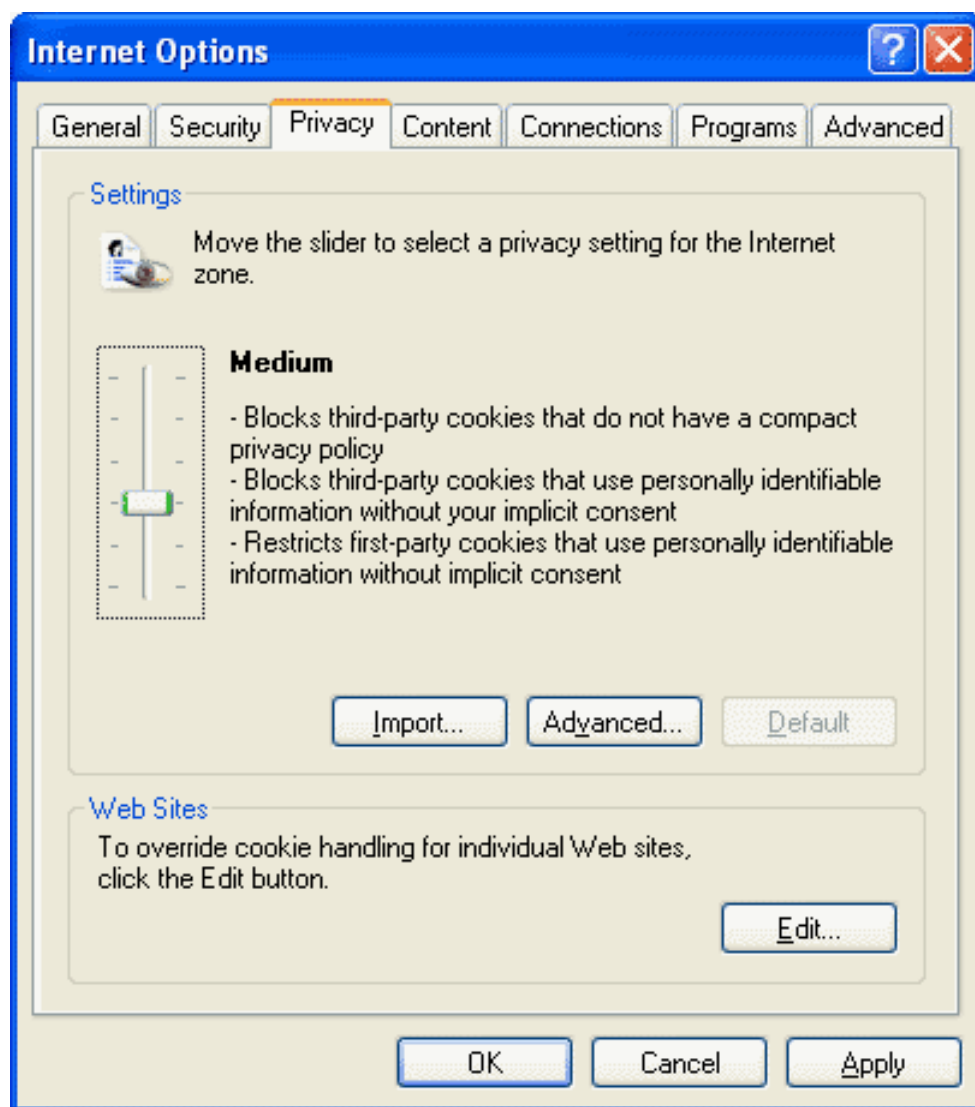
- P3P clients can check a privacy policy each time it changes
- P3P clients can check privacy policies on all objects in a web page, including ads and invisible images

<http://www.att.com/accessatt/>

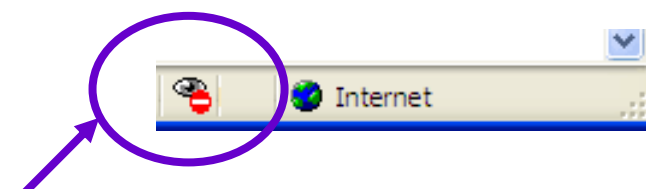


<http://adforce.imgis.com/?adlink|2|68523|1|146|ADFORCE>

P3P in IE6



Automatic processing of compact policies only:
third-party cookies without compact policies blocked by default



Privacy icon on status bar indicates that a cookie has been blocked - pop-up appears the first time the privacy icon appears



Users can click on privacy icon for list of cookies; privacy summaries are available at sites that are P3P-enabled

The screenshot shows a Microsoft Internet Explorer window displaying the GigaLaw.com website. A "Privacy Report" dialog box is open, showing a list of cookies blocked by the browser. The dialog box includes a "Show:" dropdown menu set to "Restricted Web sites" and a "Summary" button. A purple circle highlights the dialog box, and a purple arrow points to the privacy icon in the status bar.

Privacy Report

Based on your privacy settings, some cookies were restricted or blocked.

Show:

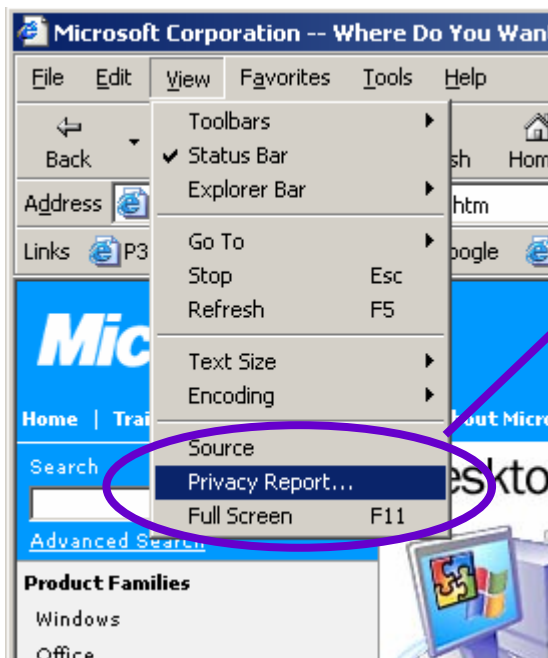
Web sites with content on the current page:

Site	Cookies
http://rcm.amazon.com/e/cm?t=gigalawcom&l=st1&...	Blocked
http://rcm-images.amazon.com/images/P/00286422...	Blocked
http://rcm-images.amazon.com/images/G/01/rcm/1...	Blocked

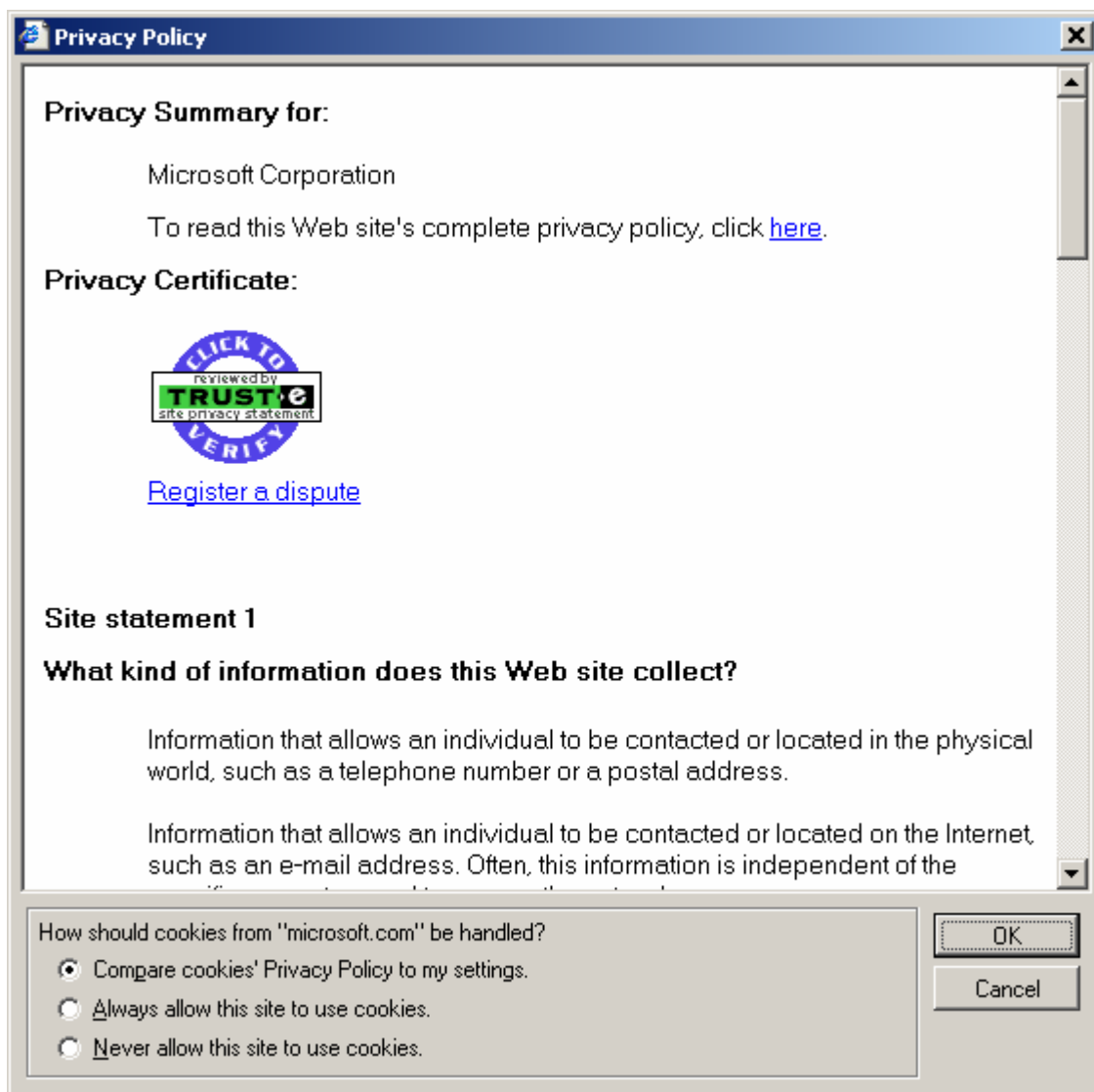
To view a site's privacy summary, select an item in the list, and then click Summary.

[Learn more about privacy...](#)

Summary Settings... Close

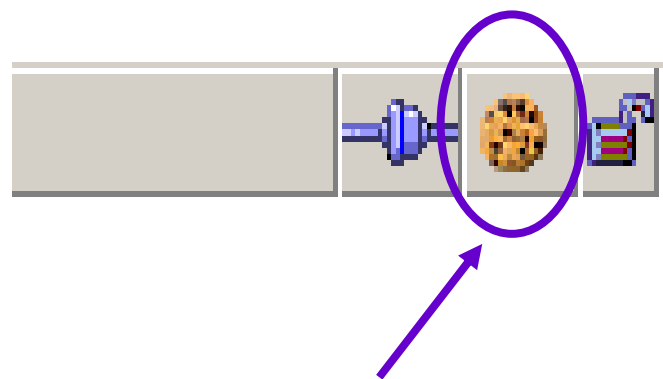
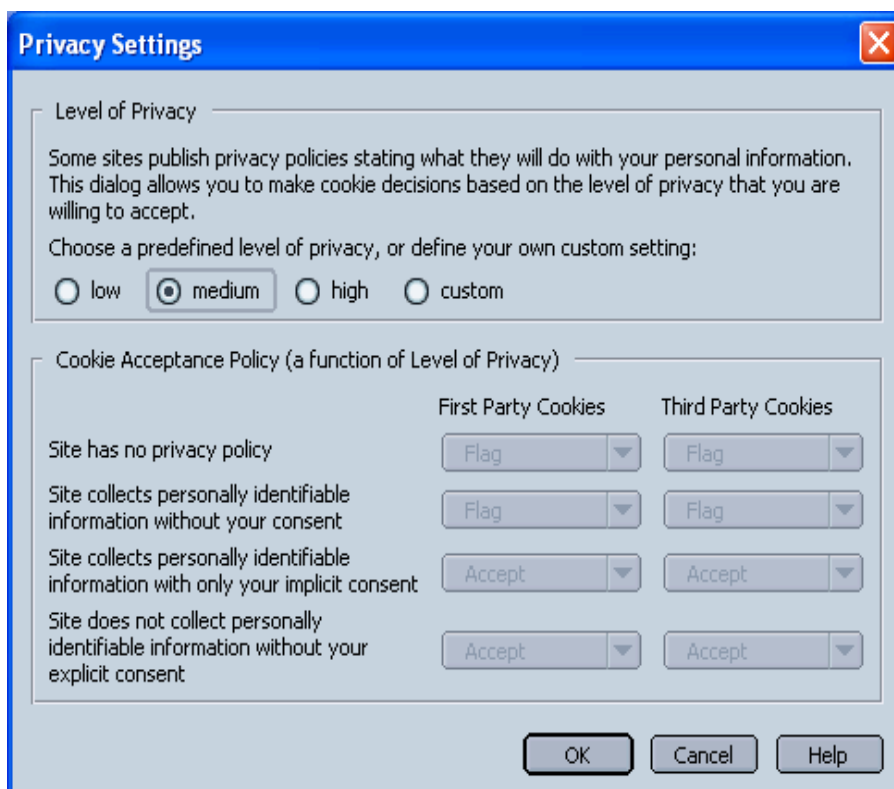


Privacy summary
report is
generated
automatically
from full P3P policy



P3P in Netscape 7

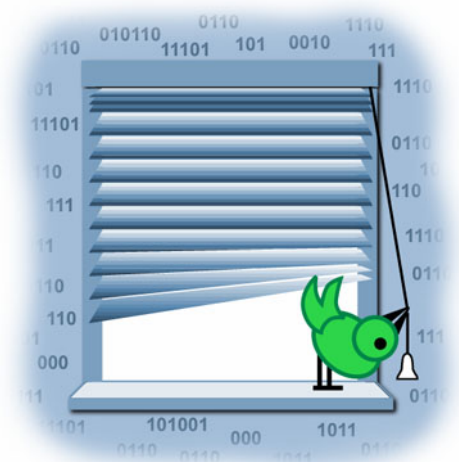
Preview version similar to IE6, focusing, on cookies; cookies without compact policies (both first-party and third-party) are “flagged” rather than blocked by default



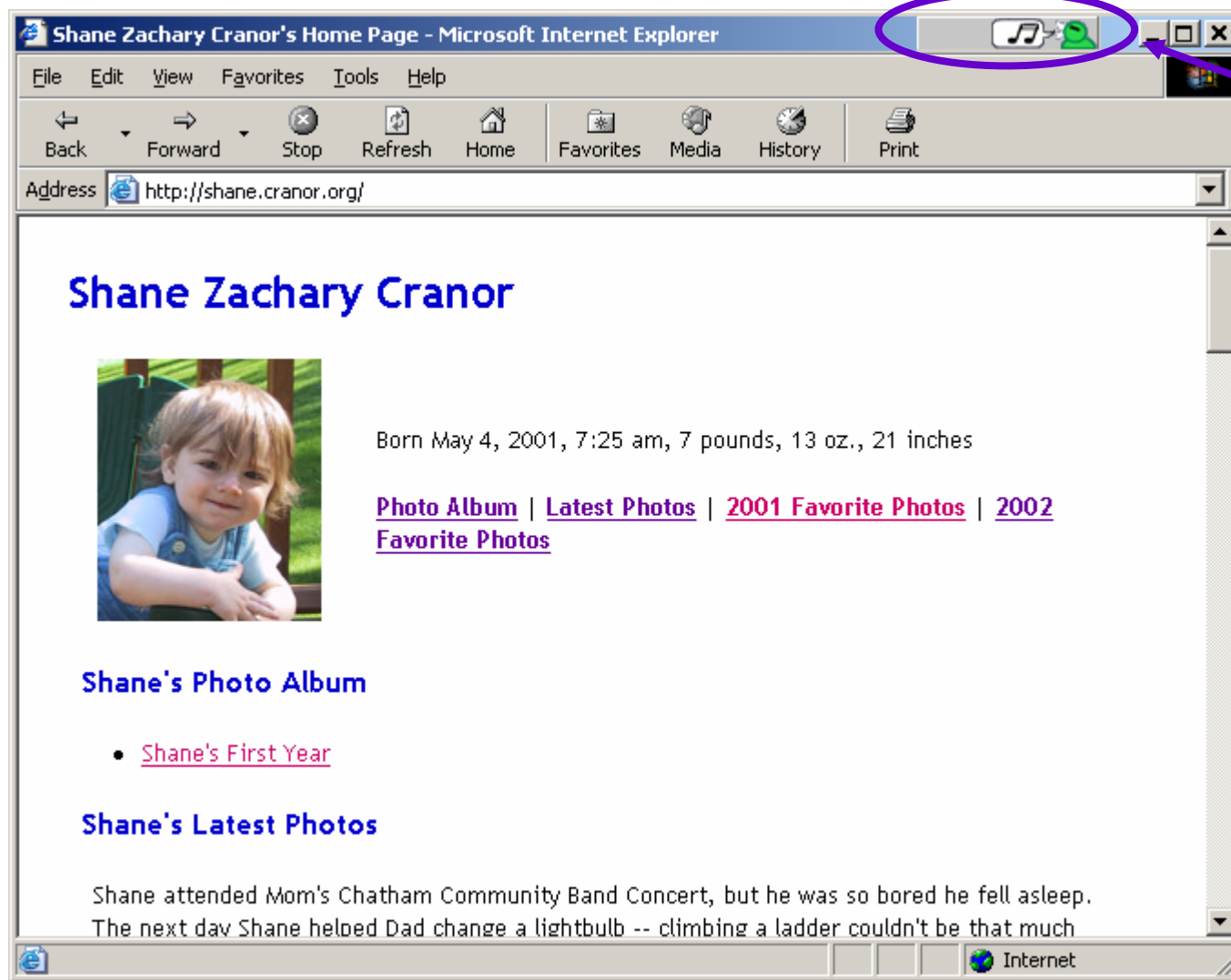
Indicates flagged cookie

AT&T Privacy Bird

- Free download of beta from <http://privacybird.com/>
- “Browser helper object” for IE 5.01/5.5/6.0
- Reads P3P policies at all P3P-enabled sites automatically
- Puts bird icon at top of browser window that changes to indicate whether site matches user’s privacy preferences
- Clicking on bird icon gives more information
- Current version is information only - no cookie blocking



Chirping bird is privacy indicator



Click on the bird for more info

The screenshot shows a Microsoft Internet Explorer window titled "Shane Zachary Cranor's Home Page - Microsoft Internet Explorer". The address bar shows "http://shane.cranor.org". The main content area displays a privacy policy summary for "Shane Cranor's Home Page Privacy Practices".

Policy Summary

Shane Cranor's Home Page Privacy Practices

Privacy Policy Check

Shane Cranor's Home Page's privacy policy *matches your preferences*.

Privacy Policy Summary

This site has the following statements in its policy:

- [Site Statement 1](#)

Site Statement 1

Types of Information Collected:

- HTTP protocol information
- Click-stream information

How your information will be used:

- Research and development
- To complete the activity for which the data was provided
- Web site and system administration

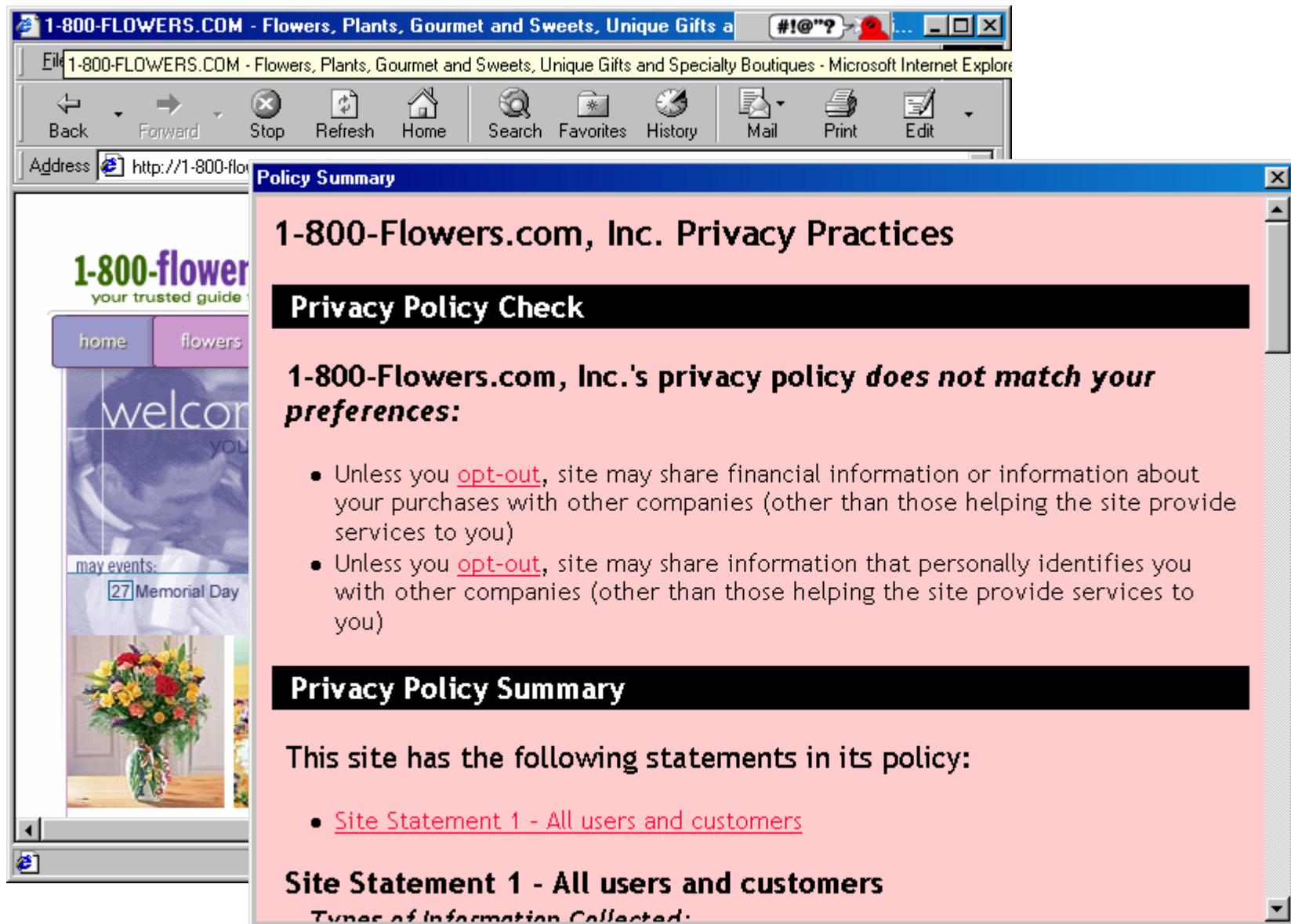
Who will use your information:

- This web site and its agents

On the left side of the browser window, there is a sidebar with a photo of a young child and links to "Shane's Photo Album" and "Shane's Latest Photos".



Privacy policy summary - mismatch



The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying <http://1-800-flowers.com>. The website content is partially visible on the left, showing the 1-800-flowers logo and a 'welcome' message. Overlaid on the right is a 'Policy Summary' dialog box with a pink background. The dialog box contains the following text:

1-800-Flowers.com, Inc. Privacy Practices

Privacy Policy Check

1-800-Flowers.com, Inc.'s privacy policy *does not match* your preferences:

- Unless you [opt-out](#), site may share financial information or information about your purchases with other companies (other than those helping the site provide services to you)
- Unless you [opt-out](#), site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

Privacy Policy Summary

This site has the following statements in its policy:

- [Site Statement 1 - All users and customers](#)

Site Statement 1 - All users and customers

Types of Information Collected:

Users select warning conditions

Privacy Preference Settings [X]

These settings control when a warning icon will be displayed at the top of your browser window. You can click on the warning icon for more information.

Select Privacy Level: ☐ Low ☐ Medium ☐ High ☒ Custom ☐ Imported

HEALTH OR MEDICAL INFORMATION

Warn me at web sites that use my health or medical information :

- ☒ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
- ☒ To share with other companies (other than those helping the web site provide services to me)

FINANCIAL OR PURCHASE INFORMATION

Warn me at web sites that use my financial information or information about my purchases :

- ☒ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
- ☒ To share with other companies (other than those helping the web site provide services to me)

PERSONALLY IDENTIFIABLE INFORMATION (name, address, phone number, email address, etc.)

Warn me at web sites that may contact me to interest me in other services or products :

- ☐ Via telephone
- ☐ Via other means (email, postal mail, etc.)
- ☒ And do not allow me to remove myself from marketing/mailling lists

Warn me at web sites that use information that personally identifies me :

- ☒ To determine my habits, interests, or other characteristics
- ☒ To share with other companies (other than those helping the website provide services to me)
- ☒ Warn me at web sites that do not allow me to find out what data they have about me

NON-PERSONALLY IDENTIFIABLE INFORMATION (demographics, interests, web sites visited, etc.)

Warn me at web sites that use my non-personally identifiable information :

- ☒ To determine my habits, interests, or other characteristics
- ☒ To share with other companies (other than those helping the website provide services to me)

Buttons: Help Import Settings Export Settings OK Cancel

Bird checks policies for embedded content

Embedded Content

The images and/or other content embedded in this web page are listed below. Some of this content may be covered by a different privacy policy than the rest of the page. Select a URL to view the privacy information related to that content.

URL	Privacy Check	Type
http://a284.g.akamai.net/f/284/987/2h/lygo.com/s.gif	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/dotline_1...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/foot_angl...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_shop_...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_shop_...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_topics...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/hp_topics...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/news_Bu...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/s.gif	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/tools_ang...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/tools_righ...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/tools_righ...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/topics_do...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/ly/0/hp/valentine...	Unknown	Image
http://a676.g.akamai.net/f/676/987/12h/lygo.com/s.gif	Unknown	Image
http://hb.lycos.com/header?Z=142153&VID=1401&LHM=0&LHS=8	Matched	IFrame
http://ln.doubleclick.net/adi/ly.ln/f/h=f;pos=1;sz=468x60;tile=1;ord=10...	Matched	IFrame
http://lygo.com/ly/0/hp/s.gif	Unknown	Image
http://m.doubleclick.net/viewad/718598-buybooks468.gif	UnMatched	Image
http://www.lycos.com/css/genesis_ie.css	Matched	StyleShee

Buttons: Help, Policy Summary, View P3P Source, Close

P3P deployment overview

1. Create a privacy policy
2. Analyze the use of cookies and third-party content on your site
3. Determine whether you want to have one P3P policy for your entire site or different P3P policies for different parts of your site
4. Create a P3P policy (or policies) for your site
5. Create a policy reference file for your site
6. Configure your server for P3P
7. Test your site to make sure it is properly P3P enabled

One policy or many?

- P3P allows policies to be specified for individual URLs or cookies
- One policy for entire web site (all URLs and cookies) is easiest to manage
- Multiple policies can allow more specific declarations about particular parts of the site
- Multiple policies may be needed if different parts of the site have different owners or responsible parties (for example, different congressional offices)

Policy reference files (PRF)

- Allows web sites to indicate which policy applies to each resource (URL or cookie)
 - ★ Every resource (HTML page, image, sound, form action URL, etc.) can have its own policy
- User agents can cache PRFs (as long as permitted by **EXPIRY**) so they don't have to fetch a new PRF every time a user clicks

Third-party content

- Third-party content should be P3P-enabled by the third-party
- If third-party content sets cookies, IE6 will block them by default unless they have P3P compact policy
- Your first-party cookies may become third-party cookies if your site is framed by another site, a page is sent via email, etc.

Generating a P3P policy

■ Edit by hand

- ★ Cut and paste from an example

■ Use a P3P policy generator

- ★ Recommended: IBM P3P policy editor

<http://www.alphaworks.ibm.com/tech/p3peditor>

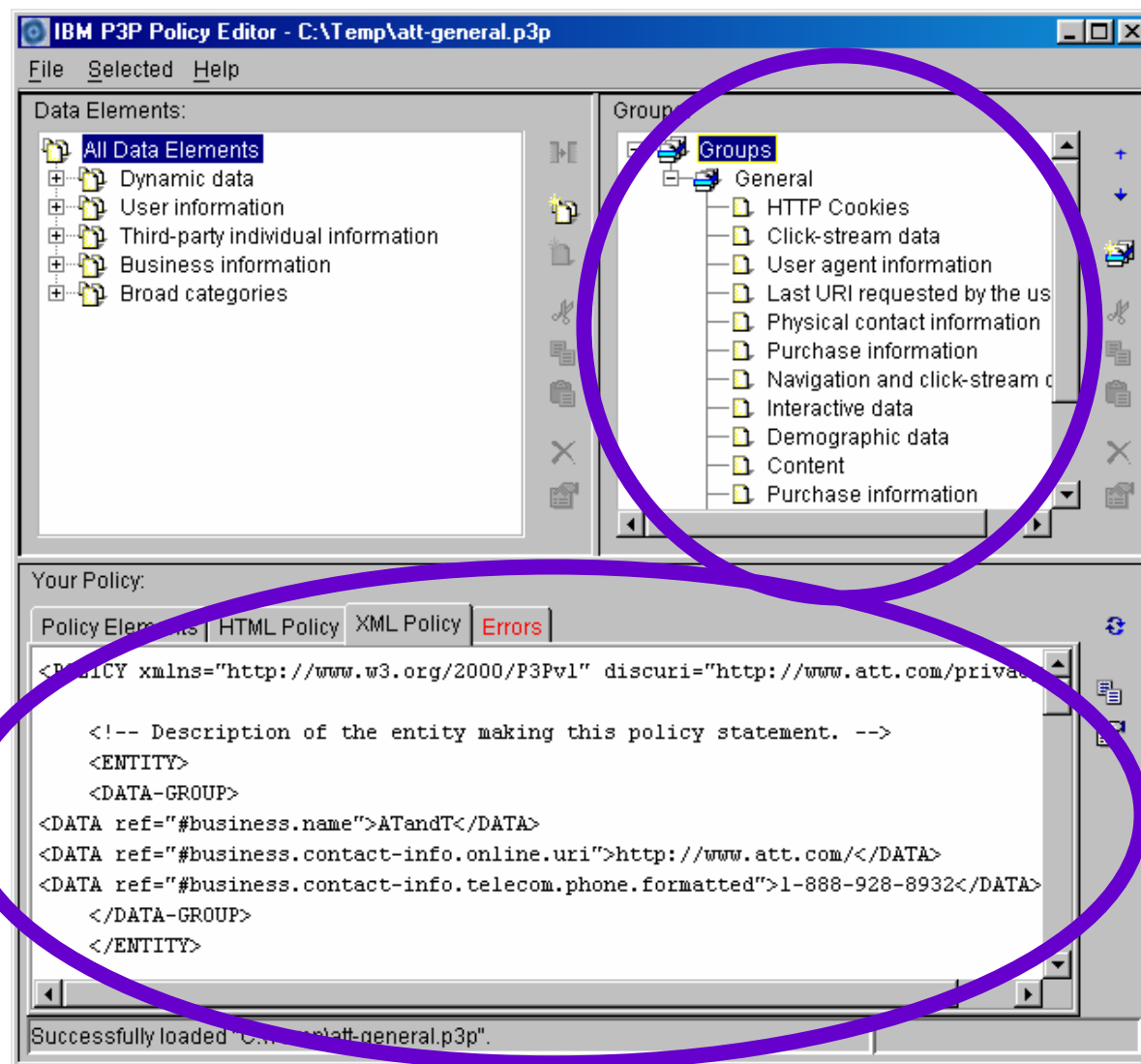
■ Generate compact policy and policy reference file the same way (by hand or with policy editor)

■ Get a book

- ★ *Web Privacy with P3P*
by Lorrie Faith Cranor

<http://p3pbook.com/>

IBM P3P Policy Editor



Sites can
list the types
of data they
collect

And view the
corresponding
P3P policy

Locating the policy reference file

- Place policy reference file in “well known location” /w3c/p3p.xml
 - ★ Most sites will do this
- Use special P3P HTTP header
 - ★ Recommended only for sites with unusual circumstances, such as those with many P3P policies
- Embed link tags in HTML files
 - ★ Recommended only for sites that exist as a directory on somebody else's server (for example, some congressional representative websites - <http://www.house.gov/NAME/>)

Server configuration

- Only needed for compact policies and/or sites that use P3P HTTP header
- Need to configure server to insert extra headers
- Procedure depends on server - see *P3P Deployment Guide* appendix
<http://www.w3.org/TR/p3pdeployment>
or Appendix B of *Web Privacy with P3P*

Policy updates

- Changing your P3P policy is difficult, but possible
- New policy applies only to new data (old policy applies to old data unless you have informed consent to apply new policy)
- Technically you can indicate exact moment when old policy will cease to apply and new policy will apply
- But, generally it's easiest to have a policy phase-in period where your practices are consistent with both policies

P3P/XML encoding

The diagram illustrates the P3P/XML encoding structure with the following annotations:

- P3P version**: Points to the `xmlns="http://www.w3.org/2002/01/P3Pv1"` attribute in the `<POLICIES>` tag.
- Location of human-readable privacy policy**: Points to the `discuri="http://p3pbook.com/privacy.html"` attribute in the `<POLICY>` tag.
- P3P policy name**: Points to the `name="policy"` attribute in the `<POLICY>` tag.
- Site's name and contact info**: A bracket on the left side of the `<ENTITY>` block, encompassing the `<DATA-GROUP>` and `<ACCESS>` sections.
- Access disclosure**: Points to the `<ACCESS><nonident/></ACCESS>` section.
- Human-readable explanation**: Points to the `<CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>` section.
- How data may be used**: Points to the `<PURPOSE><admin/><current/><develop/></PURPOSE>` section.
- Data recipients**: Points to the `<RECIPIENT><ours/></RECIPIENT>` section.
- Data retention policy**: Points to the `<RETENTION><indefinitely/></RETENTION>` section.
- Types of data collected**: Points to the `<DATA-GROUP>` section, which contains `<DATA ref="#dynamic.clickstream"/>` and `<DATA ref="#dynamic.http"/>`.
- Statement**: A bracket on the left side of the `<STATEMENT>` block, encompassing the `<CONSEQUENCE>`, `<PURPOSE>`, `<RECIPIENT>`, `<RETENTION>`, and `<DATA-GROUP>` sections.

```

<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
  <POLICY discuri="http://p3pbook.com/privacy.html"
    name="policy">
    <ENTITY>
      <DATA-GROUP>
        <DATA
          ref="#business.contact-info.online.email">privacy@p3pbook.com
        </DATA>
        <DATA
          ref="#business.contact-info.online.uri">http://p3pbook.com/
        </DATA>
        <DATA ref="#business.name">Web Privacy With P3P</DATA>
      </DATA-GROUP>
      <ACCESS><nonident/></ACCESS>
    </ENTITY>
    <STATEMENT>
      <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
      <PURPOSE><admin/><current/><develop/></PURPOSE>
      <RECIPIENT><ours/></RECIPIENT>
      <RETENTION><indefinitely/></RETENTION>
      <DATA-GROUP>
        <DATA ref="#dynamic.clickstream"/>
        <DATA ref="#dynamic.http"/>
      </DATA-GROUP>
    </STATEMENT>
  </POLICY>
</POLICIES>
  
```


Assertions in a P3P policy

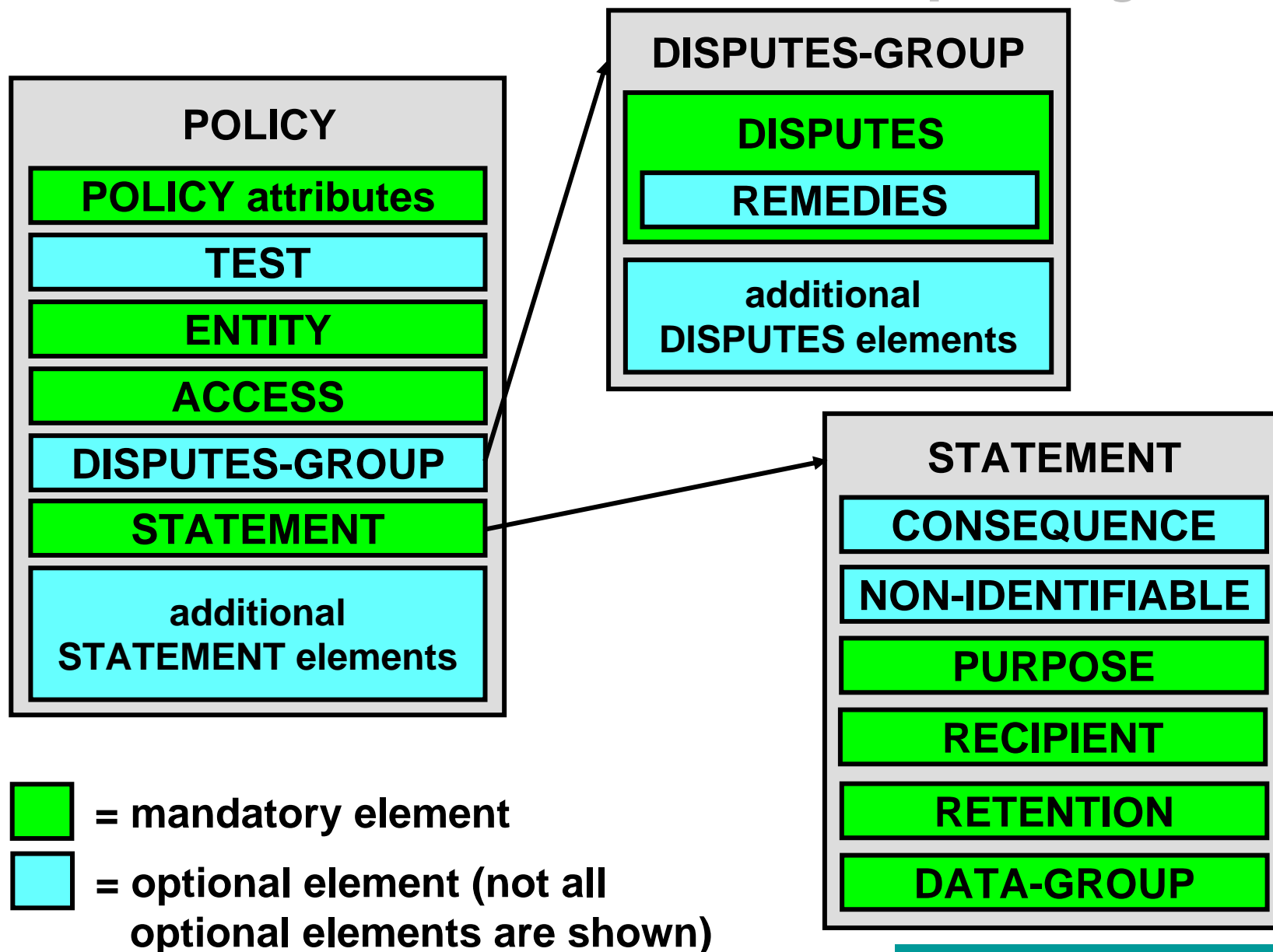
■ General assertions

- ★ Location of human-readable policies and opt-out mechanisms - **discuri**, **opturi** attributes of **<POLICY>**
- ★ Indication that policy is for testing only - **<TEST>** (optional)
- ★ Web site contact information - **<ENTITY>**
- ★ Access information - **<ACCESS>**
- ★ Information about dispute resolution - **<DISPUTES>** (optional)

■ Data-Specific Assertions

- ★ Consequence of providing data - **<CONSEQUENCE>** (optional)
- ★ Indication that no identifiable data is collected - **<NON-IDENTIFIABLE>** (optional)
- ★ How data will be used - **<PURPOSE>**
- ★ With whom data may be shared - **<RECIPIENT>**
- ★ Whether opt-in and/or opt-out is available - required attribute of **<PURPOSE>** and **<RECIPIENT>**
- ★ Data retention policy - **<RETENTION>**
- ★ What kind of data is collected - **<DATA>**

Structure of a P3P policy



Don't forget to test!

- Make sure you use the P3P validator to check for syntax errors and make sure files are in the right place
<http://www.w3.org/P3P/validator/>
 - ★ But validator can't tell whether your policy is accurate
- Use P3P user agents to view your policy and read their policy summaries carefully
- Test multiple pages on your site

P3P Validator

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Use to validate
fully P3P-enabled
site

Use to validate
P3P policy before
posting to web site

Common errors to avoid

- Failing to mention web logs in policy
- Failing to mention data linked to cookies
- Unnecessarily disclosing contact purpose
- Failing to give opturi when opt-in or opt-out are used
- Hand coding a PRF and using / or \ instead of /* to apply policy to entire site
- Omitting policy name or putting a space in the policy name
- Omitting COOKIE-INCLUDE in PRF of site with cookies
- Putting P3P files on password protected sections of site
- Failing to P3P-enable secure server
- Failing to test

Resources

■ For further information on P3P see:

- ★ <http://www.w3.org/P3P/>
- ★ <http://p3ptoolbox.org/>
- ★ <http://p3pbook.com/>

